
# Avis 37/2023 sur le projet de décision de l'autorité de contrôle compétente luxembourgeoise concernant l'approbation des exigences relatives à l'agrément d'un organisme de certification au titre de l'article 43, paragraphe 3, du RGPD

**Adopté le 21 décembre 2023**

Translations proofread by EDPB Members.
This language version has not yet been proofread.

# Table des matières

## Le comité européen de la protection des données (le «comité»),

vu l'article 63, l'article 64, paragraphe 1, point c), l'article 64, paragraphes 3 à 8, et l'article 43, paragraphe 3, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord EEE et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 10 et 22 de son règlement intérieur du 25 mai 2018,

considérant ce qui suit:

(1) Le rôle principal du comité est de garantir l'application cohérente du règlement (UE) 2016/679 (ci-après le «RGPD») dans l'ensemble de l'espace économique européen. Conformément à l'article 64, paragraphe 1, du RGPD, le comité émet un avis chaque fois qu'une autorité de contrôle compétente envisage d'approuver les exigences en matière d'agrément des organismes de certification au titre de l'article 43 dudit règlement. L'objectif du présent avis est dès lors de mettre au point une approche harmonisée concernant les exigences qu'une autorité de contrôle de la protection des données ou que l'organisme national d'accréditation appliquera aux fins de l'agrément d'un organisme de certification. Même si le RGPD n'impose pas un ensemble unique de prescriptions relatives à l'agrément, il favorise la cohérence. Le comité cherche à atteindre cet objectif dans ses avis, premièrement en encourageant les autorités de contrôle à définir leurs exigences en matière d'agrément sur la base du cadre exposé à l'annexe de ses lignes directrices relatives à l'agrément des organismes de certification, et secondement en les analysant à l'aide de son modèle de comparaison (conformément à la norme ISO IEC 17065/2012 et auxdites lignes directrices).

(2) En vertu de l'article 43 du RGPD, les autorités de contrôle compétentes adoptent des exigences en matière d'agrément. Elles appliquent toutefois le mécanisme de contrôle de la cohérence afin que le mécanisme de certification puisse susciter la confiance, notamment en fixant un niveau élevé d'exigences.

(3) Si les exigences en matière d'agrément sont soumises au mécanisme de contrôle de la cohérence, elles ne doivent pas ipso facto être identiques. Les autorités de contrôle compétentes jouissent d'une marge d'appréciation par rapport au contexte national ou régional et doivent tenir compte de leur législation locale. L'objectif de l'avis du comité n'est pas d'obtenir un ensemble unique d'exigences au sein de l'Union, mais plutôt d'éviter de graves incohérences susceptibles, par exemple, d'ébranler la confiance en l'indépendance ou en l'expertise des organismes de certification agréés.

(4) Les «Lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du règlement général sur la protection des données (2016/679)» (ci-après les «lignes directrices»), et les «Lignes directrices 1/2018 relatives à la certification et à la définition des critères

[1] Dans le présent avis, par «Union», on entend l'«EEE».

de certification conformément aux articles 42 et 43 du règlement (UE) 2016/679» serviront de fil conducteur dans le cadre du mécanisme de contrôle de la cohérence.

(5) Si un État membre exige que les organismes de certification soient agréés par l'autorité de contrôle, cette même autorité devrait établir des exigences en matière d'agrément, y compris, mais sans s'y limiter, les exigences exposées à l'article 43, paragraphe 2. Comparé aux obligations relatives à l'agrément d'organismes de certification par des organismes nationaux d'accréditation, l'article 43 contient moins d'informations quant aux exigences en matière d'agrément lorsque l'autorité de contrôle procède elle-même à l'agrément. Dans le but de contribuer à une approche harmonisée de l'agrément, les exigences en la matière appliquées par l'autorité de contrôle devraient être orientées par la norme ISO IEC 17065/2012 et être complétées par les exigences supplémentaires établies par une autorité de contrôle conformément à l'article 43, paragraphe 1, point b). Le comité fait remarquer que l'article 43, paragraphe 2, points a) à e), reflète et précise les exigences de la norme ISO IEC 17065/2012, ce qui contribuera à la cohérence[2].

(6) L'avis du comité est adopté conformément à l'article 64, paragraphe 1, point c), et à l'article 64, paragraphes 3 et 8, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur du comité, dans un délai de huit semaines à compter du premier jour ouvrable suivant la date à laquelle la présidente et l'autorité de contrôle compétente ont décidé que le dossier était complet. Sur décision de la présidente, ce délai peut être prolongé de six semaines en fonction de la complexité de la question.

**A ADOPTÉ L'AVIS SUIVANT:**

# 1 RESUME DES FAITS

1. L'autorité de contrôle luxembourgeoise a présenté au comité son projet d'exigences en matière d'agrément au titre de l'article 43, paragraphe 1, point a), du RGPD. Le dossier a été jugé complet le 26 octobre 2023. L'autorité de contrôle luxembourgeoise procédera à l'agrément des organismes de certification à certifier sur la base des critères de certification du RGPD.

2. Il s'agit du deuxième ensemble d'exigences en matière d'agrément applicables aux organismes de certification que l'autorité de contrôle luxembourgeoise soumet au comité. Conformément au projet de décision nationale de l'autorité de contrôle luxembourgeoise, la première série d'exigences en matière d'agrément soumises au comité ne s'appliquera qu'aux organismes de certification souhaitant fournir des services de certification dans le cadre du système national de certification «RGPD-CARPA», approuvé par l'autorité de contrôle luxembourgeoise le 13 mai 2022[3], ou à tout futur système de certification utilisant la norme ISAE3000 comme méthode d'audit. Sur cette première série d'exigences, le comité a émis un avis (5/2020) au titre de l'article 64, point c), du RGPD. Cet ensemble

[2] Paragraphe 39 des lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du règlement général sur la protection des données. Disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

[3] Décision nº 15/2022 de la CNPD

d'exigences a été révisé en tenant compte du présent avis de l'EDPB, conformément à l'article 10, paragraphe 8, du règlement intérieur du comité.

La deuxième série d'exigences en matière d'accréditation sera applicable aux organismes de certification qui souhaitent fournir des services de certification dans le cadre de tous les autres systèmes de certification qui n'utilisent pas la norme ISAE3000 comme méthode d'audit obligatoire. Par conséquent, le comité émet un nouvel avis sur ce nouveau sujet au titre de l'article 64, point c), du RGPD.

# 2 ÉVALUATION

## 2.1 Raisonnement général du comité concernant le projet de décision présenté

3. Le présent avis a pour objet d'évaluer les exigences en matière d'agrément établies par une autorité de contrôle, par rapport à la norme ISO 17065 ou à un ensemble complet d'exigences, afin de permettre à un organisme national d'accréditation ou à une autorité de contrôle d'agréer, conformément à l'article 43, paragraphe 1, du RGPD, un organisme de certification chargé de délivrer et de renouveler une certification conformément à l'article 42 du RGPD, et ce, sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente. Dans ce cas spécifique, le comité constate qu'en vertu du droit national, l'autorité de contrôle luxembourgeoise est investie de l'agrément des organismes de certification. À cette fin, ladite autorité a formulé un ensemble d'exigences destinées spécialement à l'agrément des organismes de certification, parallèlement à une liste de critères de certification qui doivent encore être officiellement approuvés.

4. La présente évaluation des exigences supplémentaires de l'autorité de contrôle tchèque en matière d'agrément a pour but d'examiner des variantes (ajouts ou suppressions) par rapport aux lignes directrices et, notamment, à son annexe 1. En outre, l'avis du comité porte également sur tous les aspects susceptibles d'avoir une incidence sur une approche harmonisée de l'agrément des organismes de certification.

5. Il y a lieu de constater que l'objectif des lignes directrices relatives à l'agrément des organismes de certification est d'aider les autorités de contrôle à définir leurs exigences en la matière. L'annexe des lignes directrices ne constitue pas une liste d'exigences en matière d'agrément proprement dites. L'autorité de contrôle doit par conséquent définir les prescriptions relatives à l'agrément des organismes de certification de sorte à garantir leur application pratique et cohérente selon sa situation.

6. Le comité reconnaît que, compte tenu de leur expertise, les organismes nationaux d'accréditation devraient bénéficier d'une liberté de manœuvre lorsqu'ils élaborent certaines dispositions spécifiques dans le cadre des exigences applicables en matière d'agrément. Le comité estime toutefois nécessaire de souligner que, lorsque des exigences supplémentaires sont établies, elles devraient être définies de manière à permettre leur application pratique et harmonisée et leur contrôle, le cas échéant.

7. Le comité relève que les normes ISO, notamment la norme ISO 17065, sont soumises à des droits de propriété intellectuelle et il ne fera dès lors pas référence au texte du document connexe dans le présent avis. Le comité a donc décidé de mentionner, le cas échéant, des parties spécifiques de la norme ISO, sans toutefois en reproduire le libellé.

8. Enfin, le comité a procédé à son évaluation en suivant la structure visée à l'annexe 1 des lignes directrices (ci-après l'«annexe»). Lorsque le présent avis ne commente pas une section spécifique du projet d'exigences en matière d'agrément de l'autorité de contrôle luxembourgeoise, il convient de comprendre que le comité n'a aucune observation à formuler et qu'il ne demande pas à ladite autorité de prendre des mesures supplémentaires.

9. Le présent avis ne porte pas sur les points présentés par l'autorité de contrôle luxembourgeoise qui ne relèvent pas du champ d'application de l'article 43, paragraphe 2, du RGPD, comme les références à la législation nationale. Le comité indique néanmoins que la législation nationale devrait être conforme au RGPD lorsque cela est nécessaire.

## 2.2 Principales questions d'intérêt (article 43, paragraphe 2, du RGPD et annexe 1 des lignes directrices du comité) prévues dans les exigences en matière d'agrément devant faire l'objet d'une évaluation cohérente

a. Traitement de l'ensemble des domaines clés décrits dans l'annexe des lignes directrices, et examen de tout écart par rapport à cette annexe.

b. Indépendance de l'organisme de certification.

c. Conflits d'intérêts de l'organisme de certification.

d. Expertise de l'organisme de certification.

e. Garanties appropriées pour veiller à l'application correcte des critères de certification par l'organisme de certification.

f. Procédures en vue de la délivrance, de l'examen périodique et du retrait d'une certification délivrée en vertu du RGPD.

g. Traitement transparent des réclamations relatives aux violations de la certification.

10. Compte tenu du fait que:

a. l'article 43, paragraphe 2, du RGPD établit une liste des domaines d'agrément qu'un organisme de certification doit aborder pour être agréé;

b. l'article 43, paragraphe 3, du RGPD prévoit que les exigences en matière d'agrément des organismes de certification sont approuvées par l'autorité de contrôle compétente;

c. l'article 57, paragraphe 1, points p) et q), du RGPD prévoit qu'une autorité de contrôle compétente doit rédiger et publier les exigences en matière d'agrément des organismes de certification et peut décider de procéder elle-même à l'agrément des organismes de certification;

d. l'article 64, paragraphe 1, point c), du RGPD dispose que le comité émet un avis chaque fois qu'une autorité de contrôle envisage d'adopter les exigences en matière d'agrément d'un organisme de certification conformément à l'article 43, paragraphe 3;

e. si l'organisme national d'accréditation procède à l'agrément conformément à la norme ISO/IEC 17065/2012, les exigences supplémentaires établies par l'autorité de contrôle compétente doivent également être appliquées;

f. l'annexe 1 des lignes directrices relatives à l'agrément des organismes de certification contient des suggestions d'exigences que l'autorité de contrôle de la protection des données rédige et qui s'appliquent durant l'agrément d'un organisme de certification par l'organisme national d'accréditation;

le comité est de l'avis exposé ci-après:

### 2.2.1 REMARQUES GÉNÉRALES

11. Le comité reconnaît que l'autorité de contrôle luxembourgeoise fait référence à la norme «ISO/IEC 17065:2012» dans la partie introductive, mais aussi ultérieurement dans le projet d'exigences (par exemple, dans la section 2 «référence normative», section 2 «termes et définitions»). Le comité encourage l'autorité de contrôle luxembourgeoise à citer systématiquement cette appellation dans l'ensemble des exigences en matière d'agrément.

12. De même, le comité constate que les termes «cible de l'évaluation» sont définis à la section 3 des exigences en matière d'agrément de l'autorité de contrôle luxembourgeoise. Toutefois, dans d'autres parties des exigences, telles que la section 6.1.1.4, l'autorité de contrôle luxembourgeoise fait référence à l'«objet de l'évaluation» au lieu de faire référence à la «cible de l'évaluation». À des fins de cohérence et afin d'éviter toute confusion, le comité encourage l'autorité de contrôle luxembourgeoise à utiliser ces termes de manière cohérente dans l'ensemble du libellé des exigences.

13. En ce qui concerne la section 3 relative aux «termes et définitions», le comité se félicite du fait que l'autorité de contrôle luxembourgeoise définisse les termes «exigences en matière d'accréditation» comme «les exigences établies par l'autorité de surveillance compétente par rapport auxquelles une accréditation est effectuée et qui ne sont pas basées sur la norme EN-ISO/IEC 17065/2012». Étant donné que ces exigences supplémentaires s'ajoutent à celles du RGPD, le comité encourage l'autorité de contrôle luxembourgeoise à remplacer l'expression «qui sont fondées sur» par «en plus de» afin de refléter plus clairement le fait que ces exigences s'ajoutent à celles découlant du RGPD.

14. En ce qui concerne la définition de la cible de l'évaluation, le comité encourage l'autorité de contrôle luxembourgeoise à mettre cette définition en conformité avec les lignes directrices, en ajoutant que les opérations de traitement pertinentes peuvent inclure les données à caractère personnel traitées, les systèmes techniques utilisés et les processus et procédures connexes.

15. Dans un souci de cohérence et afin d'éviter toute confusion, le comité encourage l'autorité de contrôle luxembourgeoise à remplacer le phrasé «une organisation que l'organisme de certification certifie», à la section 4.2.6 de son projet d'exigences, par le terme «client», tel que défini dans la section «termes et définitions» des exigences.

16. Le comité constate que l'autorité de contrôle luxembourgeoise, dans la section 3 «modalités et conditions» du projet d'exigences en matière d'agrément, fait référence, en plus des définitions découlant des lignes directrices, aux définitions figurant dans le RGPD, telles que celle du responsable du traitement, du sous-traitant et des données à caractère personnel. Afin de limiter la possibilité de

confusion et d'interprétation de ces définitions par l'organisme de certification, le comité encourage l'autorité de contrôle luxembourgeoise à supprimer le texte des définitions et, lorsqu'elle fait référence aux responsables du traitement, aux sous-traitants et à d'autres termes du RGPD, à se référer plutôt à l'article 4 du RGPD et à la disposition correspondante.

### 2.2.2 EXIGENCES GÉNÉRALES EN MATIÈRE D'AGRÉMENT

17. À la section 4.1.1.1 de son projet d'exigences en matière d'agrément, l'autorité de contrôle luxembourgeoise prévoit que «l'organisme de certification est en mesure de démontrer à la CNPD qu'il respecte les présentes exigences en matière d'agrément ainsi que le RGPD en sa qualité à la fois d'organisme de certification et de responsable du traitement/sous-traitant». L'organisme de certification doit être à même de prouver que ses procédures et mesures sont conformes au RGPD en ce qui concerne spécifiquement le contrôle et le traitement des données à caractère personnel dans le cadre des activités de certification. Le comité encourage l'autorité de contrôle luxembourgeoise à modifier cette exigence en conséquence.

18. Il note qu'à la section 4.2.1 du projet d'exigences en matière d'agrément de l'autorité de contrôle luxembourgeoise concernant la gestion de l'impartialité, il est précisé que l'organisme de certification doit fournir une preuve distincte de son impartialité. Les lignes directrices font référence à la preuve de l'indépendance. Le comité encourage l'autorité de contrôle luxembourgeoise à modifier ce point conformément aux lignes directrices.

19. Dans la même section du projet d'exigences en matière d'agrément de l'autorité de contrôle luxembourgeoise, le comité note que l'organisme de certification doit établir et communiquer des politiques et des procédures. Toutefois, le projet d'exigences n'indique pas clairement qui sera le destinataire de ces politiques et procédures. Par conséquent, le comité encourage l'autorité de contrôle luxembourgeoise à préciser dans son projet d'exigences que ces politiques et procédures seront communiquées en les mettant à la disposition de l'autorité de surveillance ainsi que du personnel concerné, qui devra s'y conformer.

20. Le comité prend note du fait que l'autorité de contrôle luxembourgeoise indique, à la section 4.3.1.a du projet d'exigences, que l'organisme de certification, outre les exigences énoncées à la page 4.3.1 de la norme ISO 17065, veille régulièrement à évaluer les risques liés à ses activités de certification. Toutefois, pour le comité il n'est pas clair à quels risques cette évaluation se rapporte. Par souci de clarté, le comité encourage l'autorité de contrôle luxembourgeoise à préciser dans les exigences que les risques visés sont des risques financiers.

21. Dans la même section, à la lettre b), du projet d'exigences en matière d'agrément de l'autorité de contrôle luxembourgeoise, le comité encourage cette dernière à ajouter que les mesures appropriées ne se rapportent pas uniquement à l'assurance, mais également aux réserves financières, conformément aux lignes directrices.

22. À la section 4.5.4 de son projet d'exigences en matière d'agrément, l'autorité de contrôle luxembourgeoise indique que «[l]'organisme de certification établit des politiques et des procédures destinées à préserver la confidentialité, la sauvegarde sécurisée, l'intégrité, l'accessibilité et la possibilité de récupérer les documents d'engagement». Afin d'éviter toute confusion et à des fins de cohérence, le comité encourage l'autorité de contrôle luxembourgeoise à préciser que ces termes ont

la même signification que les termes «confidentialité, intégrité et disponibilité» ou à remplacer les termes actuellement utilisés par ces derniers, issus des lignes directrices.

23. En ce qui concerne la même section du projet d'exigences en matière d'agrément de l'autorité de contrôle luxembourgeoise, le comité note que l'expression «documentation relative à l'engagement» est incluse. Le comité encourage l'autorité de contrôle luxembourgeoise soit à définir cette expression dans la section «termes et définitions», soit à inclure une expression plus claire qui faciliterait la compréhension de cette exigence par l'organisme de certification.

### 2.2.3 EXIGENCES RELATIVES AU PROCESSUS

24. Le comité note que la section 7.2.1, point b), du projet d'exigences en matière d'agrément de l'autorité de contrôle luxembourgeoise («demande») contient une référence au(x) contrat(s) entre le responsable du traitement et le sous-traitant ainsi qu'à leurs modalités spécifiques. Tout en reconnaissant que l'autorité de contrôle luxembourgeoise a repris le libellé de l'annexe, le comité l'invite à inclure également une référence aux responsables conjoints du traitement et à leurs accords spécifiques, conformément à l'article 26 du RGPD.

## 3 CONCLUSIONS/RECOMMANDATIONS

25. Le comité a évalué le projet d'exigences en matière d'agrément de l'autorité de surveillance luxembourgeoise et n'a identifié aucun problème susceptible d'entraîner une application incohérente de l'agrément des organismes de contrôle.

## 4 OBSERVATIONS FINALES

26. Le présent avis est adressé à l'autorité de contrôle luxembourgeoise et sera publié conformément à l'article 64, paragraphe 5, point b), du RGPD.

27. Conformément à l'article 64, paragraphes 7 et 8, du RGPD, l'autorité de contrôle luxembourgeoise fait savoir à la présidente du comité par voie électronique, dans un délai de deux semaines suivant la réception de l'avis, si elle maintiendra ou si elle modifiera son projet de liste. Dans le même délai, elle fournit le projet de liste modifié ou, si elle n'a pas l'intention de suivre l'avis du comité, en tout ou en partie, elle fournit les motifs pertinents pour lesquels elle n'a pas l'intention de suivre cet avis.

28. L'autorité de contrôle luxembourgeoise communique la décision finale au comité en vue de son inclusion dans le registre des décisions ayant fait l'objet d'un examen dans le cadre du mécanisme de contrôle de la cohérence, conformément à l'article 70, paragraphe 1, point y), du RGPD.

Pour le comité européen de la protection des données

La présidente

(Anu Talus)



Adopté